I CLAIM:

1. A system for processing of information over a network comprising:

at least first and second processing devices and an interface, the first processing device transmitting a communication having a desired destination being the second processing device, the first processing device also transmitting security information associated with the communication, the communication and security information being received by the interface, , the interface processing the security information and communication to identify an authorized or unauthorized condition, the interface transmitting the communication to the second processing device on identification of an authorized condition.

2. The system of claim 1, wherein the interface compares the security information against stored security information and transmits the communication to the second processing device where there is a match between the security information and stored security information.

3. The system of claim 2, wherein the stored security information is located in a database .

4. The system of claim 2, wherein the security information comprises biometric information.

5. The system of claim 1, further comprising a storage device containing the security information in electronic form that is communicated to the first processing device.

6. The system of claim 5, wherein the storage device comprises a card, the first and second processing devices comprises a computer and the interface comprise a server.

7. The system of claim 6, further comprising a reader in communication with the first processing device and adapted to upload the security information from the card and download the security information onto the first processing device.

8. The system of claim 6, wherein the first processing device transmits the communication and security information over a network.

9. The system of claim 8, wherein the network comprised the internet .

10. The system of claim 8, further comprising a GPS tracking device on at least one of said card, reader or computer for providing location information.

11. The system of claim 10, wherein the card comprises a plurality of compartments, in which each compartment contains different information and requires a different unique pin code for access thereto.

12. The system of claim 11 in which said card displays a photo image of the person assigned to said card.

13. The system of claim 12 in which said card contains in a compartment a digitized photo image of the person assigned to said card.

14. The system of claim 13 in which one of said compartments contains biometric identifying information about the assigned user of said card.

15. The system of claim 8, wherein the communication comprises an electronic mail communication .

16. The system of claim 15, wherein the biometric information selected from the group consisting of facial characteristics, finger prints, DNA, and retina characteristics.

17. Software for use in a system for information processing,

the system comprising:

a storage device containing identifying information;

a first processing device receiving the identifying information from the storage device and transmitting the identifying information over a network; and

an interface receiving the identifying information from the first processing device;

the software comprising:

an element for enabling the interface to conduct a comparison of the identifying information against stored identifying information.

18. The software of claim 17, further comprising an element for enabling the interface to transmit information to a second processing device where there is a match between the received identifying information and stored identifying information.

19. The software of claim 18, further comprising an element for transmitting a communication from the first processing device associated with the transmitted identifying information.

20. The software of claim 19, wherein the identifying information comprises biometric information.

21. The software of claim 20, further comprising an element for basing the transmitted identifying information on the biometric information.

22. The software of claim 21, wherein the storage device comprises a card, the first and second processing devices comprises a computer and the interface comprise a server.

23. The software of claim 22, wherein the network comprises the internet.

24. The software of claim 22, further comprising an element for basing the identifying information transmitted from the first processing device on location information of the first processing device.

25. The software of claim 24, wherein the location information comprises an IP address.

26. The software of claim 24, further comprising a GPS tracking device on at least one of said card, a reader for uploading identifying information from the card that is downloaded onto the first processing device or the first processing device , for providing the location information.

27. The software of claim 24, wherein the card comprises a plurality of compartments, in which each compartment contains different information and requires a different unique pin code for access thereto.

28. The software of claim 27 in which said card displays a photo image of the person assigned to said card.

29. The software of claim 28 in which said card contains in a compartment a digitized photo image of the person assigned to said card.

30. The software of claim 29 in which one of said compartments contains biometric identifying information about the assigned user of said card.

31. The software of claim 22, wherein the software further comprises an element to detect communication selected from the group consisting of viruses or worms..

32. The software of claim 31, wherein the biometric information is selected from the group consisting of facial characteristics, finger prints, DNA, and retina characteristics.

33. The software of claim 26, further comprising an element for enabling the reader to extract information from said card from specific compartments, with the reader having a unique pin code associated with a particular compartment on said card so that a pre-selected reader can only extract information from a compartment for which said pre-selected reader has the proper pin code associated with that compartment.

34. A method of information processing comprising:

Storing identifying information on a card;

reading the stored identifying information from said card;

creating an authentication mark based on the stored identifying information;

transmitting information along with the authentication mark ;

receiving the information along with the authentication mark at a first destination;

verifying whether the information is authorized based on the authentication mark; and

transmitting authorized information to a second destination.

35. A method of claim 34, further comprising measuring actual identifying information, comparing the measured actual identifying information against the stored identifying information and transmitting the information and authentication mark where there is a match between the measured actual identifying information and stored identifying information.

36. The method of claim 34, wherein the identifying information comprises biometric information.

37. The method of claim 36, further comprising basing the authentication mark on the biometric information.

38. The method of claim 37 further comprising providing a reader for reading the stored identifying information, a biometric device for measuring the actual biometric information and a computer for transmitting the information and authentication mark over a network.

39. The method of claim 38, further comprising basing the authentication mark on location information of the computer.

40. The method of claim 39, wherein the location information comprises at least one of an IP address of the computer or a GPS tracking device on at least one of said card, reader or computer for providing the location information.

41. The method of claim 40 further comprising transferring of the authentication mark and information transmitted from the computer to one or more target computers external to the computer .

42. The method of claim 41 further comprising regulating access to the one or more target computers based on the authentication mark.

43. The method of claim 37, wherein verifying whether the information is authorized based on the authentication mark comprising comparing the biometric information from the authentication mark against stored biometric information.